УДК 004.4:004.056.53

Субботин А.М., Умницын М.Ю.

ПОДХОД К КОНФИГУРИРОВАНИЮ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПОД ЗАДАННЫЕ ТРЕБОВАНИЯ

Аннотация. Статья посвящена разработке программного комплекса для конфигурирования системы защиты информации от несанкционированного доступа под заданные требования. Она описывает программный комплекс, который позволяет настраивать СЗИ от НСД для правильной работы под заданные требования.

Ключевые слова: информационная безопасность, СЗИ от НСД, Dallas Lock, настройка.

Abstract. The article is devoted to the development of software package for configuring information security means against unauthorized access according specified requirements. It describes a software package that allows you to configure information security means for correct operation according specified requirements.

Keywords: information security, information security means, unauthorized access, Dallas Lock, setting.

Введение

Становление информационного общества связано с широким распространением персональных компьютеров, построением глобальной информационной Сети и подключения к ней большого числа пользователей. Эти достижения должны коренным образом изменить жизнь общества, выдвинув на передний план деятельность, связанную с производством, потреблением, трансляцией и хранением информации.

Одной из наиболее серьезных проблем, затрудняющих применение информационных технологий, является обеспечение информационной безопасности.

Данные СЗИ от НСД занимают более 75% рынка, однако уровень поддержки DallasLock и наличия наработанных шаблонов по их конфигурированию (в виду более динамичного развития) несколько ниже, чем у основного конкурента. У начинающих специалистов часто возникают проблемы с настройкой данных средств защиты, согласно требованиям нормативной документации. И если в документации SecretNet приведены настройки, которые необходимо настраивать по разным нормативным документам, для семейства DallasLock таких наработок нет.

При аттестации АС чаще всего приходится настраивать СЗИ от НСД для защиты персональных данных, конфиденциальной информации, государственной тайны.

Информационные системы персональных данных (ИСПДн), согласно 5 пункту Постановления №1119 подразделяются на 4 группы, по количеству на 2 категории, по угрозам на 3 категории.

Для удобства определения уровня защищенности воспользуйтесь следующей таблицей, которая сделана на основе ПП-1119.

Таблица 1 – Определение уровня защищенности по категориям ПДн

Тип ИСПДн	*Сотрудники оператора*	*Количество субъектов*	*Тип актуальных угроз*		
			1 (НДВ ОС)		
ИСПДн-С (специальные)	Нет	> 100 000	УЗ-1	ИСПДн-С (специальные)	Нет
	Нет	< 100 000	УЗ-1		Нет
	Да				Да
ИСПДн-Б (биометрические)			УЗ-1	ИСПДн-Б (биометрические)	
ИСПДн-И (иные)	Нет	> 100 000	УЗ-1	ИСПДн-И (иные)	Нет
	Нет	< 100 000	УЗ-2		Нет
	Да				Да
ИСПДн-О (общедоступные)	Нет	> 100 000	УЗ-2	ИСПДн-О (общедоступные)	Нет
	Нет	< 100 000	УЗ-2		Нет

Основные признаки группировки в различные классы связаны с:

- наличием в АС информации различного уровня конфиденциальности; уровнем полномочий субъектов доступа АС на доступ к конфиденциальной информации; режимом обработки данных в АС (коллективный или индивидуальный).

Для каждого класса сформулирован определенный набор требований для подсистем:

– управления доступом;

– регистрации и учета;

– криптографической;

обеспечения целостности.

Согласно [1], группа 1 классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов: 1Д, 1Г, 1В, 1Б и 1А.

Группа 2 классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса: 2Б и 2А.

Группа 3 классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса: 3Б и 3А.

Данные документы содержат похожие требования, что унифицирует конфигурацию устройств при разных целях защиты информации. Анализ общих требования приведен в таблице 2.

Таблица 2 – Анализ нормативно-правовых актов в области защиты информации, регламентирующих требования защиты

РУКОВОДЯЩИЙ ДОКУМЕНТ. «АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ. КЛАССИФИКАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ»	**РУКОВОДЯЩИЙ ДОКУМЕНТ. «СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ. ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ»**	**ПРИКАЗ ОТ 18 ФЕВРАЛЯ 2013 Г. N 21 «ОБ УТВЕРЖДЕНИИ СОСТАВА И СОДЕРЖАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ»**
Идентификация и аутентификация субъектов доступа и объектов доступа		
Регистрация событий безопасности		
Взаимодействие пользователя с КСЗ		
Обеспечение целостности информационной системы и персональных данных		
Наличие администратора (службы) защиты безопасности		
Тестирование		
Использование сертифицированных средств защиты		
Управление потоками информации	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	
Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей		Ограничение программной среды
Сигнализация попыток нарушения защиты	Изоляция процессов (выполнение программ) в выделенной области памяти	
Учет носителей информации	Маркировка документов	Учет машинных носителей персональных данных
Криптографическая подсистема	Защита ввода и вывода на отчуждаемый физический носитель информации	
Шифрование конфиденциальной информации	Сопоставление пользователя с устройством	Антивирусная защита
Использование аттестованных (сертифицированных) криптографических средств	Надежное восстановление	Обнаружение вторжений
Физическая охрана средств вычислительной техники и носителей информации	Контроль модификации	
Наличие средств восстановления СЗИ НСД	Контроль дистрибуции	Контроль (анализ) защищенности персональных данных

С учетом исходных данных об информационной системе необходимо учитывать:

- уровень защищенности ИСПДн (определяет базовый набор мер по обеспечению безопасности ПДн);
- структурно-функциональные характеристики (адаптируют базовый набор мер);
- уже внедренные в ИСПДн СЗИ;
- необходимость технической поддержки,
- получить перечень СЗИ на выходе, функционал которых полностью компенсируют предъявляемые требования к ИСПДН.

В результате анализа настроек и требований в DallasLock 8.0-C выделяются следующие настройки. Однако Dallas Lock имеет средства импорта\экспорта настроек. Настройки хранятся в конфигурационном файле *.dls, который можно импортировать/экспортировать с помощью главного меню Dallas Lock.

Таблица 3 – Анализ структуры файла настроек СрЗИ

Группа	Определение	Количество параметров
LogonPolicy	Политика входа в систему: устанавливает требования к процессу идентификации и аутентификации	20
AuditPolicy	Политика аудита: перечень событий подлежащих аудиту	34
IntegrityPolicy	Политика целостности: перечень программных и аппаратных ресурсов подлежащих контролю целостности	31
NetAccessKeys	Ключи сетевого входа	3
IsolatedProcesses	Изолированные процессы: защищенная программная среда	1
CommonParameters	Общие параметры: кол-во пользователей и настройки системы	2
UserSection	Раздел описания пользователей ОС	10
GroupSection	Раздел описания групп ОС.	2
SessionsExclusions	Сессии-исключения	59
UserRightSection	Раздел прав пользователя	26
ResourceAccessDescription	Описание доступа к ресурсам	1
ResourceAccessDescription	Описание доступа к ресурсам	6
MandatNames	Название меток доступа в мандатной модели разграничения доступа	5
ClearingPolicy	Политика очистки остаточной информации	5
RmvKeys	Ключи преобразования сменных носителей	1
DeviceAccess	Политика доступа к устройствам (глобальные параметры)	290
DeactiveMode	Неактивный режим	1

Таблица 4 – Соответствие настроек СЗИ настройкам нормативных документов

Требования	Группа	Настройка Dallas Lock 8.0
Идентификация и аутентификация субъектов доступа и объектов доступа	LogonPolicy	Администратор Dallas Lock – Параметры безопасности – Категории – Вход – Пароли:
Регистрация событий безопасности	AuditPolicy	Администратор Dallas Lock – Параметры безопасности – Категории – Аудит
Взаимодействие пользователя с КСЗ	О/М	
Обеспечение целостности информационной системы и персональных данных	IntegrityPolicy	Администратор Dallas Lock – Параметры безопасности – Категории – Контроль целостности – Подкатегории – Политики
Наличие администратора (службы) защиты безопасности	О/М	
Тестирование	-	Администратор Dallas Lock – Верхний левый значок – Тестирование функционала СЗИ
Использование сертифицированных средств защиты	О/М	
Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	MandatNames	Администратор Dallas Lock – Учетные записи – Субъекты доступа – Учетные записи – Правая кнопка мыши на пользователя – Свойства
Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	ClearingPolicy	Администратор Dallas Lock – Параметры безопасности – Категории – Очистка остаточной информации
Сигнализация попыток нарушения защиты	auditpolicy	Администратор Dallas Lock – Параметры безопасности – Категории – Вход
Учет носителей информации Учет машинных носителей персональных данных	ResourceAccessDescription	1) Администратор Dallas Lock – Контроль ресурсов – Контроль устройств – Устройства 2) Параметры безопасности – Преобразование сменных носителей – Правая кнопка мыши на поле – Добавить – Идентификатор – ГОСТ 28147-89 – Задать желаемый пароль
Криптографическая подсистема Шифрование конфиденциальной информации	-	Правая кнопка мыши на папку, в которой необходимо зашифровать данные – DL8.0: Закодировать – Задаете желаемый пароль
Защита ввода и вывода на отчуждаемый физический носитель информации	RmvKeys	Администратор Dallas Lock – Контроль ресурсов – Контроль устройств – Устройства
Антивирусная защита	О/М	
Надежное восстановление	-	Администратор Dallas Lock – Верхний левый значок – Резервная копия файлов СЗИ
Физическая охрана средств вычислительной техники и носителей информации	О/М	
Наличие средств восстановления СЗИ НСД	О/М	

Множество требований к защите $Tr = \{Tr_1, \dots, Tr_n\}$, где n – число требований.

Множество $S = \{S_1, \dots, S_m\}$ – множество настроек Dallas Lock.

Тогда выполнение требования при реализации настройки СЗИ можно выразить матрицей:

$$\|M(S)\| = S \times Tr = \begin{cases} 0, \text{если настройка } Dallas\ Lock \text{ не влияет на данное требование} \\ 1, \text{ если влияет на данное требование} \end{cases} \quad (1)$$

В требованиях выделяется множество классов и уровней защищенности, такое что их размерность совпадает с Tr:

$$CTR = \{CTR_1, \dots, CTR_{13}\} \quad (2)$$

такое что $|CTR_k| = |Tr|$ и им соответствуют уровни защищенности и классы автоматизированных систем, приведенные в таблице ниже:

Таблица 5 – Соответствие классов и уровней защищенности математическим индексам

Индекс	1	2	3	4	5	6	7	8	9	10	11	12
Расшифровка	УЗ1	УЗ2	УЗ3	УЗ4	1Б	1В	1Г	1Д	2А	2Б	3А	3Б

Тогда настройки под определенный уровень защищенности для указанного комплекса :

$$\|M\ (S,\ CTR_k)\| = S \times CTR_k == \begin{cases} 0, \text{ не надо настраивать по требованиям} \\ 1, \text{ надо настраивать по требованиям} \end{cases} \quad (3)$$

Архитектура программного комплекса, включает в себя следующие модули:

– Пользовательский интерфейс
– Модуль выбора требований защиты
– Модуль выработки настроек защиты
– Модуль сохранению конфигурационного файла
– База данных настроек СЗИ
– База данных параметров защиты
– Конфигурационный файл

Архитектура программного комплекса представлена на рисунке 1 (2).

Интерфейс программного комплекса представлен на рисунках 2-4.

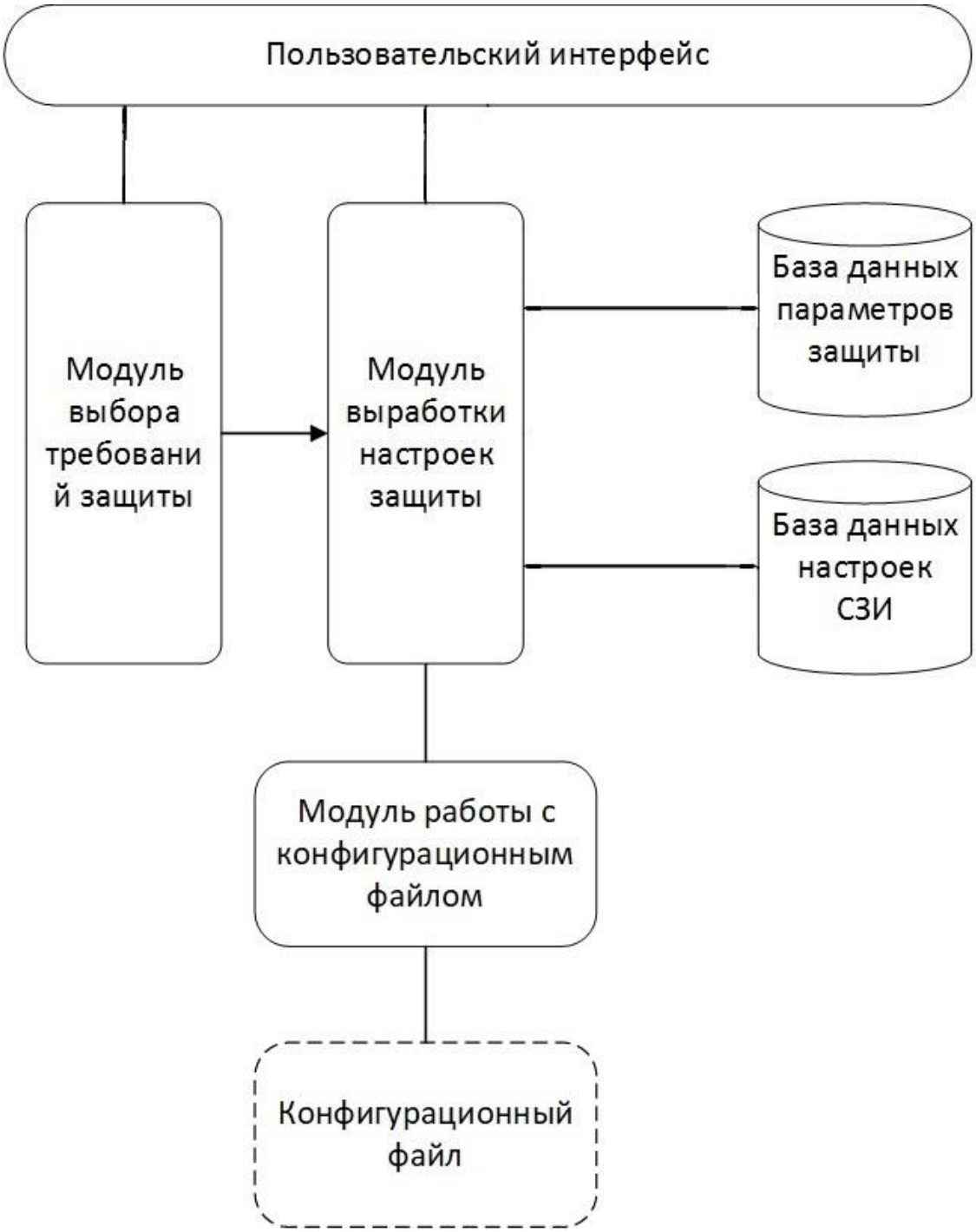

Рисунок 1 – Архитектура программного комплекса

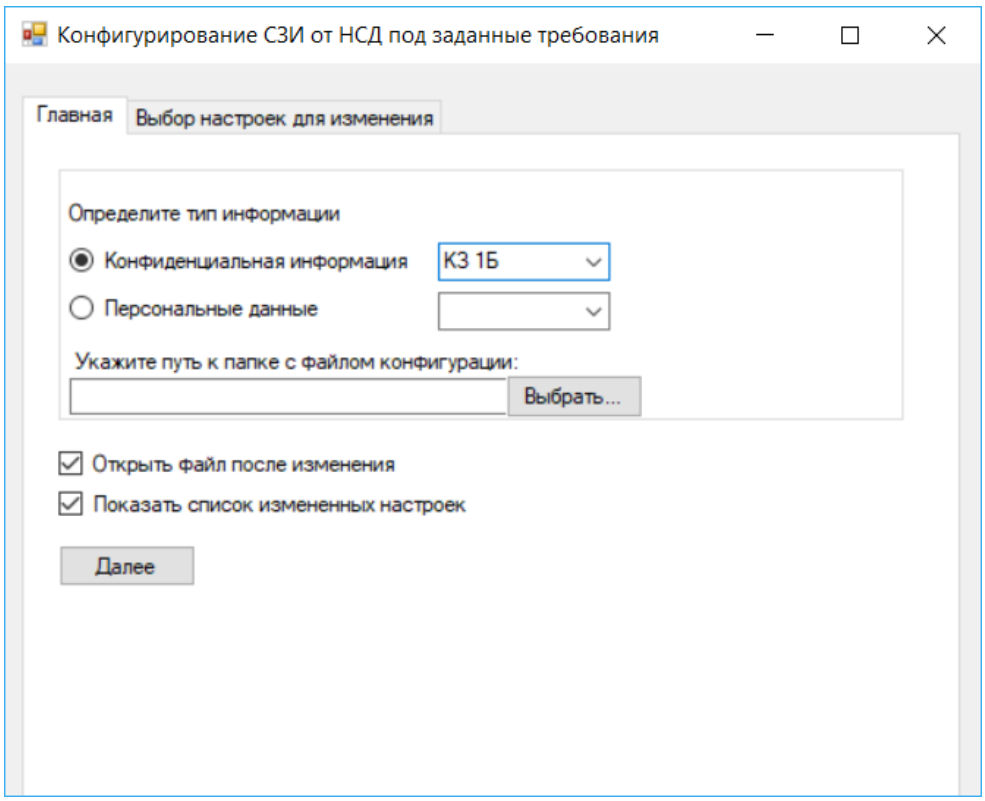

Рисунок 2 – Окно выбора типа информации и уровня конфиденциальности

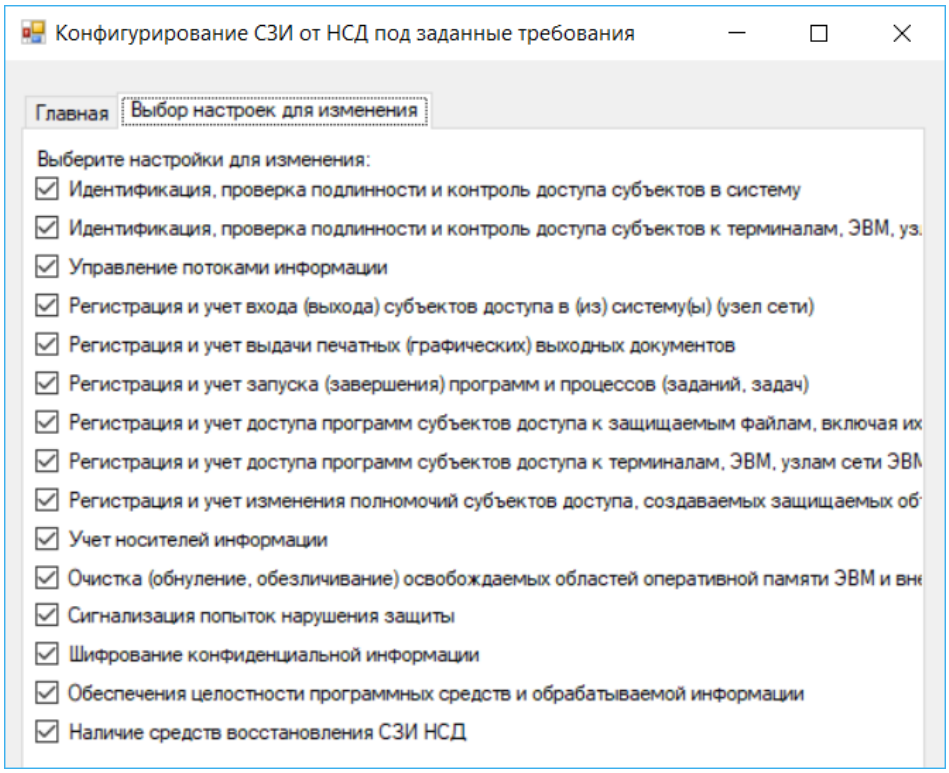

Рисунок 3 – Окно выбора настроек СрЗИ от НСД, подлежащих изменению

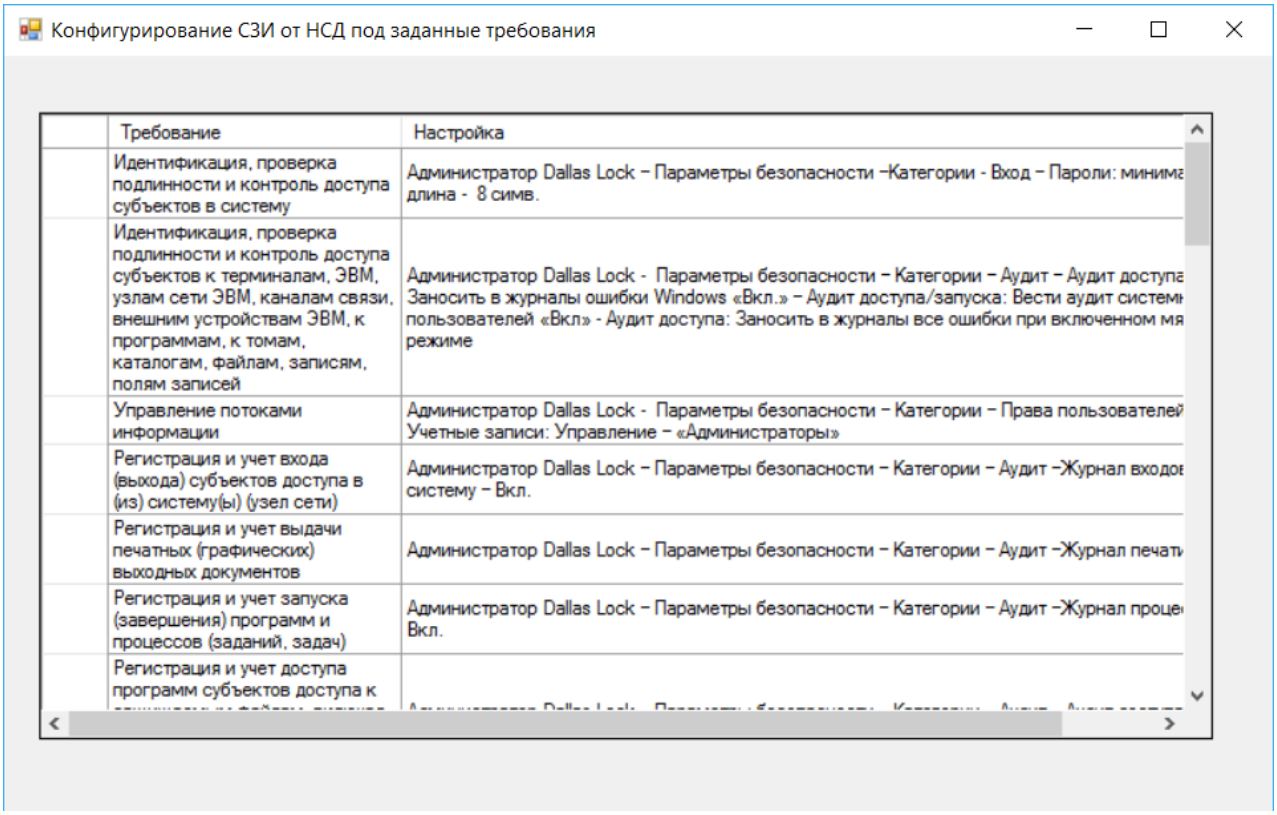

Рисунок 4 – Окно вывода настроек СрЗИ от НСД под заданные требования

В результате экспериментов было произведено конфигурирование с использованием разработанной модели и программного комплекса. Также конфигурирование выполняла контрольная группа, состоящая из студентов Волгоградского Государственного Университета группы ИБС-131.

Таблица 6 – Время выполнения экспериментов с помощью программного комплекса и контрольной группы

Эксперименты	Время конфигурирования (мин.)			
	С помощью программного комплекса		С помощью программного комплекса	
Эксперимент 1	3	Эксперимент 1	3	Эксперимент 1
Эксперимент 2	3	Эксперимент 2	3	Эксперимент 2
Эксперимент 3	3	Эксперимент 3	3	Эксперимент 3
Эксперимент 4	3	Эксперимент 4	3	Эксперимент 4

Таблица 7 – Количество ошибок, сделанных во время экспериментов с помощью программного комплекса и контрольной группы

Эксперименты	Количество ошибок			
	С помощью программного комплекса		С помощью программного комплекса	
Эксперимент 1	0	Эксперимент 1	0	Эксперимент 1
Эксперимент 2	0	Эксперимент 2	0	Эксперимент 2
Эксперимент 3	0	Эксперимент 3	0	Эксперимент 3
Эксперимент 4	0	Эксперимент 4	0	Эксперимент 4

Заключение

Разработан программный комплекс конфигурирования системы защиты информации от несанкционированного доступа под заданные требования. Система, реализующая предложенную модель, позволяет настраивать СЗИ от НСД Dallas Lock 8.0-С под заданные требования. При этом обеспечивается минимальная стоимость. Разработанная система может применяться как компонент системы управления информационной безопасностью предприятия.

Библиографический список

1. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] : приказ ФСТЭК России от 18 февр. 2013 г. № 21 // Федеральная служба по техническому и экспортному контролю : ФСТЭК : сайт. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691.
2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] : постановление Правительства Рос. Федерации от 01.11.2012 № 1119. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/.
3. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс] : руководящий док. // Федеральная служба по техническому и экспортному контролю : ФСТЭК : сайт. – Режим доступа: fstec.ru/component/attachments/download/296.
4. Ликбез по персональным данным. № 11. Уровни защищенности персональных данных [Электронный ресурс] // Центр безопасности данных. – 2012. – Режим доступа: https://data-sec.ru/personal-data/protection-level/.
5. Малкиев М. Как определить уровень защищенности информационных систем [Электронный ресурс] / М. Малкиев // Контур : электрон. журн. – 2015. – Режим доступа: https://kontur.ru/articles/1940.
6. Система защиты от несанкционированного доступа Dallas Lock 8.0 [Электронный ресурс] : рук. по эксплуатации // Конфидент : группа компаний. – 2016. – Режим доступа: https://www.dallaslock.ru/upload/medialibrary/cp/documents/RU.48957919.501410-02%2092%20-%20%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE%20%D0%BF%D0%BE%20%D1%8D%D0%BA%D1%81%D0%BF%D0%BB%D1%83%D0%B0%D1%82%D0%B0%D1%86%D0%B8%D0%B8.pdf.
7. О сертификации средств защиты информации [Электронный ресурс] : постановление Правительства Рос. Федерации от 26.06.1995 № 608. – Режим доступа: http://www.pravo.gov.ru/proxy/ips/?searchres=&x=0&y=0&bpas=cd00000&a3=&a3type=&a3value=&a6=&a6type=&a6value=&a15=&a15type=&a15value=&a7type=1&a7from=&a7to=&a7date=26.06.1995&a8=608&a8type=2&a1

=&a0=&a16=&a16type=&a16value=&a17=&a17type=&a17value=&a4=&a4type=&a4value=&textpres=&sort=7.

8. О лицензировании деятельности по технической защите конфиденциальной информации [Электронный ресурс] : постановление Правительства Рос. Федерации от 15.08.2006 № 504. – Режим доступа: http://www.garant.ru/products/ipo/prime/doc/12048955/.
9. Об информации, информационных технологиях и о защите информации (с изм. на 18 дек. 2018 г. [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ. – Режим доступа: http://sk5-410-lib-te.at.urfu.ru/docs/.